3GPP TSG SA 3 meeting #11
Mainz, Germany, 22-24 February 2000

***Document* S3-000128**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

33.102	**CR**		Current Version:	3.3.1

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	SA 7	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)*	(U)SIM	X	ME	X	UTRAN / Radio	X	Core Network	

Source: Siemens Atea **Date:** 24-01-00

Subject: Ciphering

Work item: Security

Category: *(only one category shall be marked with an X)*

F	Correction		**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature	X		Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: Clause 6.6 on ciphering is updated with the description that was in TS 33.105 and in TS 25.301. The description in 6.3.3.1 on the selection of a cipher key for user data and signalling data is moved to 6.6.6. In 6.6.5 more detail is added on how the HFN is initialised by means of the parameter START and synchronisation is maintained throughout the connection.

Clauses affected: 6.3.3.1, 6.6

Other specs affected:

Other 3G core specifications		→ List of CRs:	
Other GSM core specifications		→ List of CRs:	
MS test specifications		→ List of CRs:	
BSS test specifications		→ List of CRs:	
O&M specifications		→ List of CRs:	

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

6.3.3.1 Cipher key selection

Because of the separate mobility management for CS and PS services, the USIM establishes cipher keys with both the CS and the PS core network service domains. The conditions on the use of these cipher keys in the user and control planes are given below.

6.3.3.1.1 User plane

The CS user data connections are ciphered with the cipher key CK_{CS} established between the user and the 3G CS core network service domain and identified in the security mode setting procedure. The PS user data connections are ciphered with the cipher key CK_{PS} established between the user and the 3G PS core network service domain and identified in the security mode setting procedure.

6.3.3.1.2 Control plane

When a security mode setting procedure is performed, the cipher/integrity key set by this procedure is applied to the signalling plane, what ever core network service domain is specified in the procedure. This may require that the cipher/integrity key of an (already ciphered/integrity protected) ongoing signalling connection is changed. This change should be completed within five seconds.

6.6 Access link data confidentiality

6.6.1 General

User data and some signalling information elements are considered sensitive and must be confidentiality protected. To ensure identity confidentiality (see ~~clause~~ 6.1), the ~~Temporary~~ temporary ~~Mobile User~~ user ~~Identity~~ identity (P-)TMSI must be transferred in a protected mode at allocation time and at other times when the signalling procedures permit it. ~~The confidentiality of user traffic concerns the information transmitted on traffic channels.~~

These needs for a protected mode of transmission are fulfilled by a confidentiality function which is applied on dedicated channels between the ~~MS~~ UE and the RNC.

6.6.2 Layer of ciphering

The ciphering function is performed either in the RLC sub-layer or in the MAC sub-layer, according to the following rules:

- If a logical channel is expected to be supported on a common transport channel and has to be ciphered, it shall use UM RLC mode and ciphering is performed at the RLC sub-layer.
- If a logical channel is using a non-transparent RLC mode (AM or UM), ciphering is performed in the RLC sub-layer.
- If a logical channel is using the transparent RLC mode, ciphering is performed in the MAC sub-layer (MAC-d entity).

Ciphering when applied is performed in the S-RNC and the UE and the context needed for ciphering (CK, HFN, etc.) is only known in S-RNC and the UE.

~~6.6.2 Ciphering algorithm~~

6.6.3 Ciphering method

~~Algorithm UEA is implemented in both the MS and the RNC.~~ Figure 6.6.1 illustrates the use of the ciphering algorithm f8 to encrypt plaintext by applying a keystream using a bit per bit binary addition of the plaintext and the ciphertext. The plaintext may be recovered by generating the same keystream using the same input parameters and applying a bit per bit binary addition with the ciphertext.

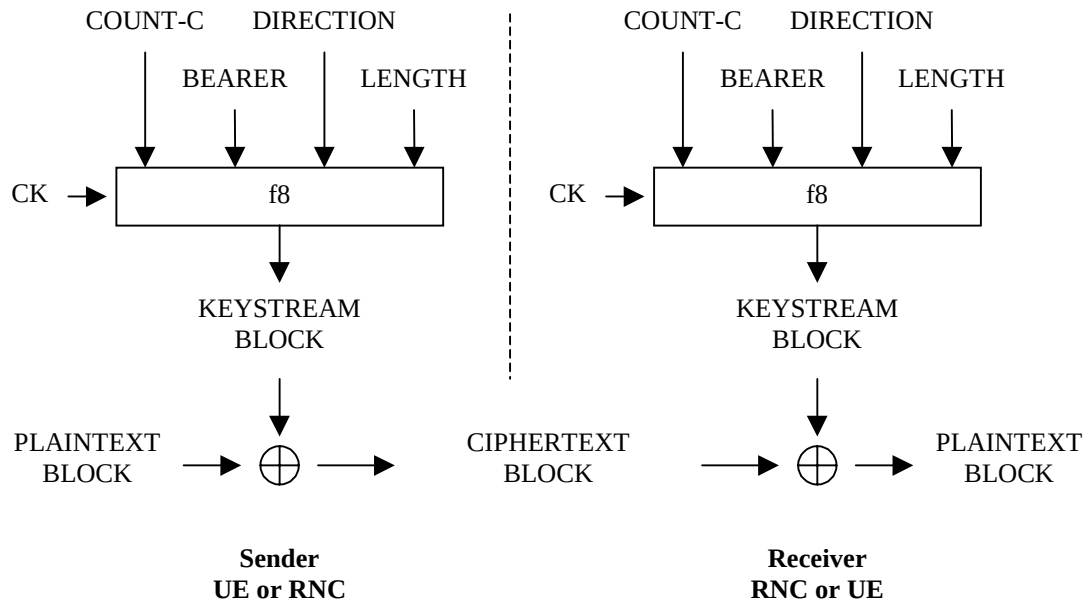

Figure 6.6.1: Ciphering of user and signalling data transmitted over the radio access link

The input parameters to the algorithm are the cipher key CK, a time dependent input COUNT-C, the bearer identity BEARER, the direction of transmission DIRECTION and the length of the keystream required LENGTH. Based on these input parameters the algorithm generates the output keystream block KEYSTREAM which is used to encrypt the input plaintext block PLAINTEXT to produce the output ciphertext block CIPHERTEXT.

The input parameter LENGTH shall affect only the length of the KEYSTREAM BLOCK, not the actual bits in it.

~~On the RNC side the description below assumes that one algorithm UEA is implemented for each dedicated physical channel [not yet decided]. The data flow on dedicated channels is ciphered by a bit per bit or stream cipher generated by an algorithm UEA.~~

6.6.4 Input parameters to the cipher algorithm

6.6.4.1 COUNT-C

The ciphering sequence number COUNT-C is 32 bits long.

There is one COUNT-C value per logical RLC AM channel, one per logical RLC UM channel and one for all logical channels using the transparent RLC mode (and mapped onto DCH).

The initialisation at the start of a connection and the synchronisation of COUNT-C throughout a connection are detailed in 6.6.5.

6.6.4.2 CK

The cipher key CK is 128 bits long.

There may be one CK for CS connections (CK_{CS}), established between the CS service domain and the user and one CK for PS connections (CK_{PS}) established between the PS service domain and the user. Which cipher key to use for a particular logical channel is described in 6.6.6.

For UMTS subscribers, CK is established during UMTS AKA, as the output of the cipher key derivation function f3, available in the USIM and in HLR/AuC. For GSM subscribers that access the UTRAN, CK is established following GSM AKA and is derived from the GSM cipher key Kc, as described in 8.2.

CK is stored in the USIM and a copy is stored in the UE. CK is sent from the USIM to the UE upon request of the UE. The USIM shall send CK under the condition that 1) a valid CK is available, 2) the current value of START in the USIM is up-to-date and 3) START has not reached THRESHOLD. The UE shall delete CK from memory after power-off as well as after removal of the USIM.

CK is sent from the HLR/AuC to the VLR or SGSN and stored in the VLR or SGSN as part of the quintet. It is sent from the VLR or SGSN to the RNC in the (RANAP) security mode command. The VLR or SGSN shall assure that CK is updated at least once every 24 hours.

At handover, the CK is transmitted within the network infrastructure from the old RNC to the new RNC, to enable the communication to proceed. The cipher CK remains unchanged at handover.

6.6.4.3 BEARER

The logical channel identifier BEARER is 4 bits long.

There is one BEARER parameter per logical channel associated with the same user and multiplexed on a single 10ms physical layer frame. The logical channel identifier is input to avoid that for different keystream an identical set of input parameter values is used.

6.6.4.4 DIRECTION

The direction identifier DIRECTION is 1 bit long.

The direction identifier is input to avoid that for the keystreams for the up-link and for the down-link would use the an identical set of input parameter values.

6.6.4.5 LENGTH

The length indicator LENGTH is 16 bits long.

The length indicator determines the length of the required keystream block. LENGTH shall affect only the length of the KEYSTREAM BLOCK, not the actual bits in it. ~~The UEA shall produce one output as a sequence of keystream bits referred to as a Key Stream Segment (KSS). A KSS of length n shall be produced to encrypt a given segment of plaintext of length n. The bits of KSS are labelled KSS(0), …KSS(n-1), where KSS(0) is the first bit output from the generator. The bits in the KSS shall be used to encrypt or decrypt the data.~~

6.6.5 Synchronisation of ciphering

COUNT-C is composed of two parts: a "short" sequence number and a "long" sequence number. The update of COUNT-C depends on the transmission mode as described below (see Figure 6.6.2):

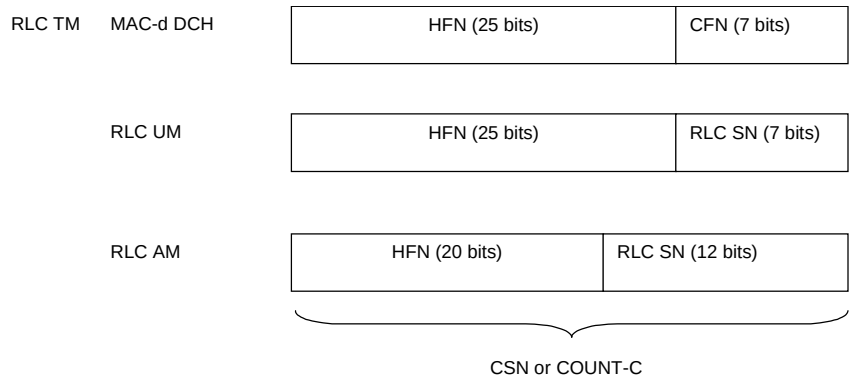

Figure 6.6.2: The structure of COUNT-C for all transmission modes

- For RLC TM on DCH, the "short" sequence number is the 7-bit ciphering frame number CFN of the UEFN. It is independently maintained in the UE MAC entity and the SRNC MAC-d entity. The "long" sequence number is the 25-bit HFN which is incremented at each CFN cycle. The ciphering sequence number CSN or COUNT-C is identical to the UEFN.

- For RLC UM mode, the "short" sequence number is the 7-bit RLC sequence number RLC SN that is available in each RLC PDU (it is not ciphered). The "long" sequence number is the 25-bit HFN which is incremented at each RLC SN cycle.

- For RLC AM mode, the "short" sequence number is the 12-bit RLC sequence number RLC SN that is available in each RLC PDU (it is not ciphered). The "long" sequence number is the 20-bit HFN which is incremented at each RLC SN cycle.

The hyperframe number HFN is initialised by means of the parameter START, which is transmitted from UE to RNC during *RRC connection establishment*. The START parameter is 25 bits long.

The UE stores a parameter START, which is equal to the highest HFN that the UE is currently using or the highest HFN that the UE has been using in the past with the current CK. If the current CK has not been used yet, then START is 0. A copy of start is stored on the USIM. During an ongoing RRC connection, only the counter in the UE is updated.

At connection establishment the UE sends an indication to the USIM. The USIM marks its START value as not up-to-date.

At connection establishment, the UE sends the START value in the *RRC connection establishment message* to the RNC. For RLC TM and RLC UM logical channels, the initial HFN is initialised to START; for RLC AM logical channels, the HFN is initialised to the 20 MSB of START. The HFN parameters are then incremented independently from one another. Throughout the RRC connection, the UE and the RNC maintain a parameter START, which is equal to the highest HFN value currently in used, incremented by 1.

When a new logical channel is created during an RRC connection, the initial value of HFN for that connection is set to the current START value (or the 20 MSB thereof).

After connection release, the UE sends the up-to-date version of START to the USIM. The USIM stores this START value and sets it as up-to-date.

When the UE is powered-on or a new USIM is inserted, the UE requests the value of START from the USIM. When the START value on the USIM is marked as up-to-date, the USIM sends it to the UE, otherwise the USIM indicates that a new authentication and key agreement is required.

6.6.6 Cipher key selection

There is one CK for CS connections (CK_{CS}), established between the CS service domain and the user and one CK for PS connections (CK_{PS}) established between the PS service domain and the user.

The logical channels for CS user data are ciphered with CK_{CS}.

The logical channels for PS user data are ciphered with CK_{PS}.

Signalling data (for both CS an PS services) is sent over common logical channels. These logical channels are ciphered by the CK of the service domain for which the most recent security mode negotiation took place. This may require that the cipher key of an (already ciphered) ongoing signalling connection is changed, when a new RRC connection establishment occurs, or when a security mode negotiation follows a re-authentication during an ongoing connection. This change should be completed within five seconds after the security mode negotiation.

6.6.~~3~~7 UEA identification

Each UEA will be assigned a 4-bit identifier. Currently the following values have been defined:

"0000_2" : UEA0, no encryption.

"0001_2" : UEA1, Kasumi.

The remaining values are not defined.

Table 2 – UEA identification

Information Element	Length	Value	Remark
UEA Number	4	0000_2	Standard UMTS Encryption Algorithm, UEA1
		0001_2	Standard UMTS Encryption Algorithm, UEA2
		0010_2	Standard UMTS Encryption Algorithm, UEA3
		0011_2 to 0111_2	Reserved for future expansion
		$1xxx_2$	Proprietary UMTS Algorithms

6.6.4 Synchronisation of ciphering

The enciphering stream at one end and the deciphering stream at the other end must be synchronised, for the enciphering bit stream and the deciphering bit streams to coincide.

Synchronisation is guarantied by driving UEA by an explicit time variable, COUNT, derived from an appropriate frame number available at the MS and at the RNC.

The diagram below summarises the implementation indications listed above, with only one enciphering/deciphering procedure represented (the second one for deciphering/enciphering is symmetrical).

6.6.4.1 Layer for ciphering

The layer on which ciphering takes place depends on the Layer 2 mode of the data. Data transmitted on logical channels using a non-transparent RLC mode (either Acknowledged Mode or Unacknowledged Mode) is ciphered in the RLC sub-layer of Layer 2. Data transmitted on a logical channel using the transparent RLC mode is ciphered at the MAC sub-layer of Layer 2.

6.6.4.2 Intra-system handover

When a handover occurs, the CK and IK are transmitted within the system infrastructure from the old RNC to the new one to enable the communication to proceed, and the synchronisation procedure is resumed. The keys CK and IK remain unchanged at handover.